UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,173	01/30/2004	Sherman (Xuemin) Chen	15415US01	7811

23446 7590 02/18/2010

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
02/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/769,173
Filing Date: January 30, 2004
Appellant(s): CHEN ET AL.

Ognyan I. Beremski
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/18/2009 appealing from the Office action mailed 6/10/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6073237	Ellison	6-2000
20020001386	Akiyama	1-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akiyama (US 2002/0001386) in view of Ellison (US 6,073,237), hereinafter Ellison.

Regarding **Claim 1**, Akiyama discloses a method for secure key authentication, the method comprising:

generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, “Digital signature”) of a secure key to obtain a digitally signed secure key (Fig. 5, “work keys”, also at paragraph 0107, “The digital signature is information used to check the authenticity of the contract information, and is used to prevent tampering.”, also at paragraph 0107, “The contract information is made up of, e.g., a receiver ID, channel contract information, the number n of work keys, n pairs of work keys and work key identifiers, and digital signature”).

encrypting the digitally signed secure key utilizing at least a previously generated unreadable secure key (Fig. 7, “Enciphered contract information”, also at Paragraph 0106, lines 5-8, “The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.”, Note:

[Each digitally signed contract information is encrypted using and master key, also note that master keys are generated and sent to clients via secure card therefore master keys are generated prior to encrypting work keys and it is also unreadable and also secure because only broadcaster and receivers have the master key (see Paragraph 0154)]

and transmitting the digitally signed and encrypted secure key from the first location (Paragraph 0167, "The transmission processing operation of an individual control packet by the information distributor apparatus shown in FIG. 29…"). Note: individual control packets contains encrypted contract information (Paragraph 0106, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7."), and as established above, contract information contains work keys, as a result, when control packet is transmitted, it contains the signed work keys as well, and thus we can interpret that signed work keys are transmitted from a broadcast device depicted in Fig. 29).

Akiyama discloses encrypting work keys with master key. Akiyama does not disclose that the master key is also encrypted and digitally signed and wherein said previously generated unreadable digitally signed and encrypted key (master key) was generated by encrypting a previously generated digitally signed secure key (master key) as now required by claim limitation.

However, using PKI system to encrypt and digitally signing the keys are well known technique in the art of cryptography, which enable secure transmission of keys over unsecured channels using asymmetric key encryption. Ellison, in the same field of

endeavor of network security, discloses encrypting and digitally signing a key wherein encryption of the key takes place after digitally signing the key (Column 4, lines 64-67, "**The session key K_x is signed by private key of the server itself K_n 121 and encrypted by the public key of the user P1e**. The encrypted and signed session key K_x is then sent back to the user 123, further note that since the encryption of session key K_x is taking place before the encryption, it reads on to the amended claim limitation that requires key to be encrypted and digitally signed wherein the digitally signed and encrypted key was generated by encrypting a digitally signed key).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, on the master key of Akiyama, a digital signature utilizing a private key of a broadcast station and then encrypt the digitally signed key with the public key of the receiver, as taught by Ellison. One of ordinary skill in the art would be motivated to do so because digital signature provides authentication and encryption provides secrecy. As a result, when the broadcast station updates the master key, it could utilize PKI technique to send new master key over an unsecured channel with fully confidentiality without having to provide each receiver a new smart card having a new master key.

Regarding **Claim 2**, the rejection of claim 1 is incorporated and further Akiyama discloses generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm (Paragraph 0111, lines 9-10, "authenticates the digital signature using key information (secret key or public key) stored in a digital signature")

Regarding **Claim 3**, the rejection of claim 1 is incorporated and the combination of Akiyama and Ellison discloses encrypting the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.") *[Each digitally signed contract information is encrypted using and master key, and Ellison discloses, as established in the rejection of claim 1 above, the limitation of encrypting a master key]*

Regarding **Claim 4**, the rejection of claim 3 is incorporated and further Akiyama discloses the secure key comprises at least one of a master key, a work key and a scrambling key. (*Fig. 5, "Work keys")*

Regarding **Claim 5**, the rejection of claim 4 is incorporated and further Akiyama discloses the receiving the digitally signed and encrypted secure key at a second location **(Paragraph 0110, lines 1-2, "Upon receiving an individual packet via the public telephone network and modem 101…")**

decrypting the digitally signed and encrypted secure key to obtain a decrypted digitally signed secure key (Paragraph 0110, Lines 11-17, "If the master key identifier matches the master key, that master key is output from the master key storage 103 (step S4) to decrypt contract information in the individual information packet")

Regarding **Claim 6**, the rejection of claim 5 is incorporated and further Akiyama discloses if the secure key comprises a work key then a decrypted digitally signed

master key at the second location is utilized for decrypting an encrypted digitally signed work key (Paragraph 0110, Lines 11-17, "If the master key identifier matches the master key, that master key is output from the master key storage 103 (step S4) to decrypt contract information in the individual information packet (step S5). Work key information (pairs of work key identifiers and work keys and the like) contained in the decrypted contract information is stored in a work key storage 105")

Regarding **Claim 7**, the rejection of claim 5 is incorporated and further Akiyama discloses if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key (Paragraph 0125, lines 9-14, "If the work key can be acquired, information of an encrypted section in the common control packet is decrypted using the work key (step S44). A channel key Kch is acquired from the decrypted information, and is stored in the channel key storage 118". Please note that channel keys are transmitted in the common control packets as shown in Fig. 8, these channel keys are encrypted by work keys as taught by paragraph 0125). The control packets are not digitally signed but Akiyama discloses use of digital signature for contract packets which is used to check the authenticity of the contract information and is used to prevent tampering. Therefore, it would have been obvious in view of Akiyama's use of digital signature in contract packets to also apply the same technique to control packets carrying channel keys. Furthermore examiner would like to point out that examiner has already provided in the rejection of claim 1 that adding a digital signature to a key to prevent tampering is obvious in vies of Ellison).

Regarding **Claim 8**, the rejection of claim 5 is incorporated and further Akiyama discloses verifying authenticity of the digital signature of the digitally signed secure key (Paragraph 0112, line 1-2, "digital signature authentication process").

Regarding **Claim 9**, the rejection of claim 8 is incorporated and further Akiyama discloses verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm (Paragraph 0111, lines 7-11, "the contract information certifying device 107 certifies or authenticates the digital signature using key information (secret key or public key) stored in a digital signature authentication key storage 108")

Regarding **Claim 10**, the rejection of claim 8 is incorporated and further Akiyama discloses determining whether to verify authenticity of the digital signature (Paragraph 0111, lines 6-8, "If the two IDs match, the contract information certifying device 107 certifies or authenticates the digital signature using key information")

Claims **11, 21 and 32** are "computer program" and "system" claims analogous to "method" claim 1. Akiyama in the same reference discloses a system for performing method of claim 1 [Broadcast receiver is depicted in figure 1 and Transmitter system is depicted in figure 29]. Also, it should be noted that since Akiyama's system discloses the hardware to perform the method of claim 1, therefore it would also have computer software that performs the method of claim 1. Claims 11, 21 and 32 are rejected under same rationale as the rejection of claim 1.

Claims **12, 22 and 33** are “computer program” and “system” claims analogous to “method” claim 2. Claims 12, 22 and 32 are rejected under same rationale as the rejection of claim 2.

Claims **13, 23 and 34** are “computer program” and “system” claims analogous to “method” claim 3. Claims 13, 23 and 34 are rejected under same rationale as the rejection of claim 3.

Claims **14, 24 and 35** are “computer program” and “system” claims analogous to “method” claim 4. Claims 14, 24 and 35 are rejected under same rationale as the rejection of claim 4.

Claims **15, 25 and 36** are “computer program” and “system” claims analogous to “method” claim 5. Claims 15, 25 and 36 are rejected under same rationale as the rejection of claim 5.

Claims **16, 26 and 37** are “computer program” and “system” claims analogous to “method” claim 6. Claims 16, 26 and 37 are rejected under same rationale as the rejection of claim 6.

Claims **17, 27 and 38** are “computer program” and “system” claims analogous to “method” claim 7. Claims 17, 28 and 38 are rejected under same rationale as the rejection of claim 7.

Claims **18, 28 and 39** are “computer program” and “system” claims analogous to “method” claim 8. Claims 18, 28 and 39 are rejected under same rationale as the rejection of claim 8.

Claims **19, 29 and 40** are “computer program” and “system” claims analogous to “method” claim 9. Claims 19, 29 and 40 are rejected under same rationale as the rejection of claim 9.

Claims **20, 30 and 41** are “computer program” and “system” claims analogous to “method” claim 10. Claims 20, 30 and 41 are rejected under same rationale as the rejection of claim 10.

Regarding **Claim 31**, rejection of claim 21 is incorporated and further Akiyama discloses at least one processor comprises at least one of a host processor, a microprocessor, and a microcontroller (Figure 29, processor used in the system of Fig. 29 is a host processor).

(10) Response to Argument

Appellant's arguments filed 11/18/2009 along with the appeal brief have been fully considered but they are not persuasive.

A. Independent claims 1, 11, 21, and 32:

- Appellant argues (see pages 7-8 of appeal brief) that, “Referring to FIG. 5 of Akiyama, the Examiner has equated Applicant's "secure key" to Akiyama's "work key", which is part of Akiyama's contract information. Furthermore, Akiyama discloses that a separate master key is used to encrypt the work key, as illustrated in FIG. 3 and further explained in paragraph 0100 of Akiyama. **However, the work keys of Akiyama are different from the master keys, which are used for encrypting the work keys. More specifically, Akiyama's**

master key is not a previously encrypted and signed work key (i.e., the master key is not generated by encrypting a previously generated signed work key). In this regard, Akiyama does not disclose that the work keys (equated by the Examiner to Applicant's "secure key") are encrypted utilizing a previously generated unreadable digitally signed and encrypted work key, where the previously generated unreadable digitally signed and encrypted work key was generated by encrypting a previously generated signed work key. In other words, Akiyama does not disclose that the work keys are encrypted using previously generated work keys, as recited in Applicant's claim 1. Ellison does not overcome the above deficiencies of Akiyama.

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "the work keys are encrypted using previously generated work keys") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key, it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a "secure key". Claim language does not require the key that encrypts the secure key to be

of same type. Furthermore appellant's own disclosure also allow the secure key to be any of master key, work key and/ or scrambling key (see claim 6 and paragraph 0028, “The secure key may be a master key, a work key and/or a scrambling key.”). Therefore, appellant argument that if examiner interpret secure key to be work key then the key that encrypts the work key needs to be work key is not found persuasive. Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection should be maintained.

B. Examiner's response to arguments:

- Appellant further argues (see, pages 9-10 of appeal brief) that, “The Applicant submits that claim 1, as presented in the 08/11/08 response, indeed required that a secure key and a key that encrypts the secure key to be of same type. However, to further prosecution and to further clarify this aspect, the Applicant amended independent claims 1, 11, 21 and 32, as set forth in the 03/02/09 response and in the claim listing below. Support for the claim amendments may be found, for example, in Fig. 6A and paragraphs 46-54 of the specification. More specifically, referring to Applicant's Fig. 6A, the digitally signed secure keys 638 are encrypted by the encryptor 608. The encrypted and signed secure keys 632 are looped back via the registers 610 and then communicated back (628 and 630) to the encryptor 608 for purposes of encrypting the next digitally signed secure key. Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the

latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys. “

- Examiner respectfully disagrees and still maintains that even Fig. 6A does not support applicant interpretation that requires secure key and key that encrypts the secure key to be of same type. See paragraph 0047 (originally filed specification) that recites ” In accordance with an aspect of the present invention, the **master decryption keys 618** may be utilized in **the encryption and decryption of one or more secure keys**, for example, a **work key and/or a scrambling key**.” Also note that claim 6 recites, “wherein if the secure key comprises a work key then a decrypted digitally signed master key at the second location is utilized for **decrypting** an encrypted digitally signed work key.”. This claim clearly establishes that when the secure key is a work key it has to be encrypted by the master key. Also see, claim 7 which recites, " wherein if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for **decrypting** an encrypted digitally signed scrambling key.”. Examiner realizes that Fig. 6A in fact shows that after encrypting the secure key do go back to encrypt the next secure keys however, as recited at paragraph 0047 and claims 6 and 7, if the work key is looped back then it will encrypt the content key. Therefore, applicant's interpretation that secure key and key that encrypts the secure key to be of same type is not consistent with the specification and dependent claims 6 and 7. Nowhere in the specification it is recited that same level keys are encrypted using the same level

keys as argued by the applicant. Also note that the current claim language does not raise rejection under U.S.C. 112 first paragraph for lacking the written description because at least one interpretation (one taken by the examiner) is supported by the specification. Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key it reads onto the claimed limitation. Further note that even though applicant is interpreting secure key and key that encrypts the secure key to be of **same type** the current language of the claim is broad enough that as long as the key that encrypt the secure key is also secure it would read onto the claims limitation. Further note that applicant's statement that "Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys" appears to be an opinion because there is no written description that requires these keys to be of **same type**. As clearly shown by paragraph 0047 and claims 6 and 7, key that encrypts the digitally signed key is chosen based on what is the type of the digitally singed key is for example if the digitally signed key is work key then master key is used to encrypt the digitally signed key and if the digitally signed key is a scrambling key then work keys are used to encrypt the digitally signed key (see, paragraph 0041 and claims 6 and 7).

- Appellant further argues (on page 10) that, "In the above citation, the Examiner refers for support to Fig. 1 and page 5, lines 22-25 of the specification. The

Examiner further states: "the invention is of a key ladder wherein lower level keys are encrypted using higher level keys. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant." The Applicant respectfully disagrees with such characterization of Applicant's invention. The Examiner is encouraged to carefully read the entire specification in light of all Figures. The Applicant is puzzled as to why the Examiner even uses Fig. 1 and page 5 of the specification to judge what Applicant's invention is, since FIGS. 1-4 were clearly marked as PRIOR ART, and pages 1-10 constitute the "Background of the Invention" section. The detailed description of the invention is in pages 15-24 and FIGS. 5-6B of the specification (the Applicant has already briefly summarized Fig. 6A and why the secure key and the key that encrypts the secure key are of the same type). As admitted (see, page 16, in the reply filed on 8/10/2009) by applicant that secure key" can be a master key, a work key, and/or, a scrambling key. The master key in Akiyama is also a type of secure key that encrypts another secure key which is a work key. Therefore, the combination still discloses the claim limitations and the rejection is maintained.

- Examiner would like to point out that examiner did rely upon Fig. 1 and page 5, lines 22-25 to establish that appellant's argument are not even supported by their own disclosure in the non-final office action mailed on 10/28/2009. After appellant argued that examiner is relying upon prior art, examiner in the final rejection (mailed on 6/10/2009) did not even mentioned those part in support of

examiner's position. Therefore examiner is not sure why appellant is bringing arguments that have already been withdrawn by examiner. Please note that in the final rejection mailed on 6/10/2009, examiner relied on paragraph 0047, fig. 6A and also claims 4, 6 and 7 to establish that appellant's argument are not even supported by their own disclosure and they are what appellant is disclosing as their invention.

- Appellant further argues (on page 14) that, Again, the issue is **not** what level keys are used by the encryptor 608 to encrypt a digitally signed secure key 638, as represented by the Examiner. The issue is how the "previously generated unreadable digitally signed and encrypted secure key" (i.e., the digitally signed and encrypted secure key 632 coming as output out of the encryptor 608, being the same as key 628 or 630) is in fact generated. In other words, regardless of whether a master key is used to encrypt a secure "work" key, the result from the encryption is an encrypted "work" key. Similarly, regardless of whether a work key is used to encrypt a secure "scrambling" key, the result from the encryption is an encrypted "scrambling" key. The encryptor 608 simply encrypts a given type of key, but the input and the output of the encryptor 608 remain the same type of key."

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "The encryptor 608 simply encrypts a given type of key, but the input and the output of the encryptor 608 remain the same type of key") are not recited

in the rejected claim(s). Although the claims are interpreted in light of the specificaion, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key, it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a "secure key". Claim language does not require the key that encrypts the secure key to be of same type. Furthermore appellant's own disclosure also allow the secure key to be any of master key, work key and/ or scrambling key (see claim 6 and paragraph 0028, "The secure key may be a master key, a work key and/or a scrambling key."). Therefore, appellant argument that if examiner interpret secure key to be work key then the key that encrypts the work key needs to be work key is not found persuasive. Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection should be maintained.

C. Rejection of Dependent Claims 2, 12, 22 and 33:

- Appellant does not submit separate arguments for claims 2, 12, 22 and 33 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

D. Rejection of Dependent Claims 3, 13, 23, and 34:

- Appellant does not submit separate arguments for claims 3, 13, 23 and 34 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

E. Rejection of Dependent Claims 4, 14, 24, and 35:

- Appellant does not submit separate arguments for claims 4, 14, 24, and 35 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

F. Rejection of Dependent Claims 5, 15, 25, and 36:

- Appellant does not submit separate arguments for claims 5, 15, 25, and 36 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

G. Rejection of Dependent Claims 6, 16, 26, and 37:

- Appellant does not submit separate arguments for claims 6, 16, 26, and 37 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

H. Rejection of Dependent Claims 7, 17, 27, and 38:

- Appellant relies on the arguments made with respect to claims 1, 11, 21, and 32 and further argues that, “The Examiner, in the above arguments, has already equated Appellant's "secure key" to Akiyama's work key in Fig. 5. However, the above cited portion of Akiyama (paragraph 0125) does not disclose that the contract information of Fig. 5 includes a scrambling key. Akiyama only discloses that the contract information of Fig. 5 includes a work key, not a scrambling key. In addition, Akiyama's step $44 does not disclose that a decrypted digitally signed work key is used for purposes of decrypting an encrypted and digitally signed scrambling key. Accordingly, the Appellant submits that claims 7, 17, 27 and 38 are allowable over the references cited in the Final Office Action at least for the above reasons.”
- In rejection of claims 7, 17, 27 and 37, examiner is equating the channel key of Akiyama to the secure key and would like to point out that the combination of

Akiyama and Ellison discloses if the secure key comprises a scrambling key (channel key) then a decrypted digitally signed work key (it is already established in the rejection of claim 1 that work keys are signed) at the second location is utilized for decrypting an encrypted digitally signed scrambling key (see, Paragraph 0125, lines 9-14, "If the work key can be acquired, information of an encrypted section in the common control packet is decrypted using the work key (step S44). A channel key Kch is acquired from the decrypted information, and is stored in the channel key storage 118". Please note that channel keys are transmitted in the common control packets as shown in Fig. 8, these channel keys are encrypted by work keys as taught by paragraph 0125). The control packets are not digitally signed but Akiyama discloses use of digital signature for contract packets which is used to check the authenticity of the contract information and is used to prevent tampering. Therefore, it would have been obvious in view of Akiyama's use of digital signature in contract packets to also apply the same technique to control packets carrying channel keys. Furthermore examiner would like to point out that examiner has already provided in the rejection of claim 1 that adding a digital signature to a key to prevent tampering is obvious in vies of Ellison). Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection should be maintained.

I. Rejection of Dependent Claims 8, 18, 28, and 39:

- Appellant does not submit separate arguments for claims 8, 18, 28, and 39 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

J. Rejection of Dependent Claims 9, 19, 29, 40:

- Appellant does not submit separate arguments for claims 9, 19, 29, 40 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

K. Rejection of Dependent Claims 10, 20, 30, and 41:

- Appellant does not submit separate arguments for claims 10, 20, 30, and 41 but relies on the arguments made with respect to claims 1, 11, 21, and 32.

L. Rejection of Dependent Claim 31:

- Appellant does not submit separate arguments for claim 31 but relies on the arguments made with respect to claim 21.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Y. P./

Examiner, Art Unit 2435

Conferees:

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435

/Ponnoreay Pich/
Primary Examiner, Art Unit 2435